VEDERE LABS

La exposición de los dispositivos y sistemas médicos en internet

Subtítulo

26 de septiembre de 2022

1. Resumen ejecutivo

El 12 de septiembre, el FBI publicó una notificación de la industria privada titulada «Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities» (Los dispositivos médicos sin parches y obsoletos ofrecen oportunidades de ciberataque). La notificación se centraba en el hecho de que un número creciente de vulnerabilidades en los dispositivos médicos puede ser explotado por actores de amenazas para «dañar las funciones operativas de los centros sanitarios, la seguridad de los pacientes, la confidencialidad y la integridad de los datos».

Esta notificación llega tras el descubrimiento de importantes vulnerabilidades que se han producido este año y que afectan dispositivos médicos como bombas de infusión, sistemas de dispensación de medicación y electrocardiógrafos, así como una oleada de ataques de ransomware dirigidos a organizaciones sanitarias en los últimos años, algunos de los cuales han inutilizado dispositivos médicos.

En este informe, analizamos por qué los dispositivos médicos son vulnerables, vamos más allá de las vulnerabilidades para ofrecer una imagen de la exposición de los dispositivos y sistemas médicos en la internet abierta, y analizamos las recomendaciones de mitigación para las organizaciones sanitarias.

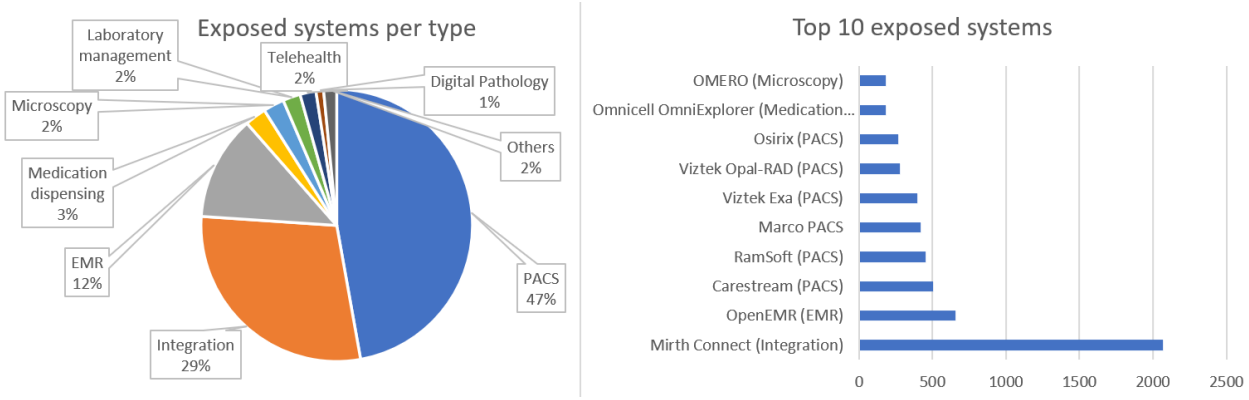
Los principales hallazgos de este informe son los siguientes:

- Encontramos más de 7000 sistemas médicos expuestos en internet, incluyendo PACS (sistemas de archivo de imágenes y comunicación), motores de integración sanitaria, EMR (registros médicos informatizados), sistemas de dispensación de medicamentos y otros. Algunos dispositivos médicos, como las impresoras de imágenes médicas, también están directamente expuestos.
- Estados Unidos tiene la gran mayoría de estos sistemas expuestos (58 % del total), seguido de Irán, India y Brasil.
- Casi la mitad de los sistemas expuestos son PACS, que se suelen basar en el protocolo DICOM para el almacenamiento y la recuperación de imágenes médicas. Si nos centramos específicamente en los sistemas DICOM, observamos 4114 sistemas expuestos, lo que supone un aumento del 14 % con respecto a hace un año.
- La aplicación de una segmentación eficaz de la red es la acción de mitigación más importante teniendo en cuenta nuestros hallazgos sobre los sistemas expuestos.

2. Un análisis de los sistemas médicos expuestos en internet

Mediante el uso de una red específica de huellas dactilares en los sistemas médicos (abiertamente accesibles para cualquiera, incluidos los atacantes), consultamos el motor de búsqueda Shodan y encontramos un total de 7168 sistemas expuestos. Más de las tres cuartas partes de los sistemas se encuentran en las Américas, y solo en Estados Unidos hay 4185 (58 % del total). La región de Asia-Pacífico y Japón (APJ) ocupa el segundo lugar, representada principalmente por India (324 sistemas expuestos) y Australia (146). Como región, Europa ocupa el tercer lugar, con la mayoría de los sistemas expuestos en Alemania (128), el Reino Unido (75) y los Países Bajos (71). Por último, en la región OMTA (Oriente Medio, Turquía y África), el país más representativo es Irán, con 427 sistemas expuestos.

Los sistemas expuestos se dividen en los siguientes tipos.



Casi la mitad de ellos son PACS, utilizados para el almacenamiento y la visualización de imágenes médicas basándose en el protocolo estándar DICOM. La segunda categoría más popular son los motores de integración sanitaria, utilizados para estandarizar los flujos de datos entre diferentes sistemas, como los datos clínicos, financieros y operativos. Estos motores suelen utilizar el protocolo estándar HL7. La tercera categoría son los sistemas de historias clínicas electrónicas (EMR), utilizados para gestionar los datos sanitarios de los pacientes. Una categoría interesante y sorprendente entre las 10 primeras es la de los sistemas de dispensación de medicamentos, que se suelen utilizar en las farmacias de los hospitales.

Si solo nos centramos en los 10 sistemas más expuestos, descubrimos que 882 de 5405 (el 16 %) tenían al menos una vulnerabilidad identificada por Shodan. Para algunos sistemas, el índice de vulnerabilidad era mucho mayor. Para Opal-RAD PACS es del 69 %, para Carestream PACS, es del 50 %, mientras que para OpenEMR es del 31 %. También es importante advertir que muchos otros sistemas podrían tener vulnerabilidades que no son identificadas automáticamente por el motor de búsqueda.

Teniendo en cuenta que los PACS son el tipo más común de sistema expuesto, decidimos estudiarlos más detenidamente. Tal y como se ha mencionado anteriormente, los sistemas PACS suelen utilizar el protocolo DICOM, por lo que podemos ampliar nuestra búsqueda para encontrar más sistemas expuestos utilizando la consulta «DICOM Server Response», que devuelve 4114 nuevos resultados. Los dispositivos que utilizan DICOM exponen el nombre (o un identificador) de la aplicación del servidor en el banner captado por Shodan. Uno de los servidores más populares encontrados en línea utiliza el OFFIS DICOM Toolkit, que recientemente, en junio, reveló un conjunto de vulnerabilidades.

3. Recomendaciones de mitigación

La notificación del FBI propone cinco categorías de acciones de mitigación para los dispositivos médicos vulnerables:

- Ejecutar la protección de los puntos finales, como el antivirus y el EDR, en aquellos dispositivos que admiten esas tecnologías.
- Utilizar contraseñas complejas y únicas por dispositivo y limitar el número de intentos de inicio de sesión.
- Mantener un inventario de dispositivos médicos y utilizarlo para la evaluación de riesgos.
- Seguir los avisos de seguridad de los proveedores y ejecutar un análisis de vulnerabilidad en los dispositivos médicos.
- Implementar una formación de seguridad para que los empleados identifiquen e informen de problemas como las amenazas internas, el *phishing* y la ingeniería social.

La notificación también anima a «tomar otras precauciones de mitigación, como aislar el dispositivo de la red o auditar las actividades de la red del dispositivo». Para obtener directrices más detalladas sobre la implementación

de la segmentación para tipos de dispositivos específicos, como PACS, EMR y bombas de infusión, consulte las publicaciones de orientación sobre seguridad del NIST. Para una orientación general sobre la evaluación de riesgos de los dispositivos médicos, véase el reciente NIST SP 800-66.

La segmentación de la red es extremadamente importante teniendo en cuenta nuestras conclusiones sobre los sistemas expuestos. Las recomendaciones del FBI, especialmente la segmentación y la supervisión de la red, no solo se deberían aplicar a los dispositivos médicos, sino a todos los dispositivos de la red de su organización. Tal y como hemos mostrado en entradas anteriores y como el Centro de Coordinación de Ciberseguridad del Sector de la Salud (HC3) ha debatido recientemente, los actores de amenazas pueden aprovechar esos otros tipos de dispositivos para obtener acceso o provocar daños a las organizaciones de salud.

Para más información y análisis técnicos lea el informe completo aquí.